## REMARKS

Claims 1, 4-11, 14-17, 19-24, and 26-30 stand rejected under 35 U.S.C. § 112, second paragraph as being indefinite. Claims 1, 4-11, 14-17, 19-24, and 26-30 stand rejected under 35 U.S.C. § 103(a) as unpatentable over United States Patent Number 7,069,434 to Ilnicki et al. (hereinafter Ilnicki) in view of United States Patent Publication 2005/0069135 by Brickell (hereinafter Brickell).

## Response to rejection under 35 U.S.C. 112

Claims 1, 4-11, 14-17, 19-24, and 26-30 stand rejected under 35 U.S.C. § 112, second paragraph as being indefinite. Applicants traverse this rejection.

Independent claim 1 includes the limitations:

> "...a secure function module configured to receive an excluding computing module context that enables the secure function module to transact secure functions with an excluding computing module comprising storing cryptographic keys for the excluding computer module;
>
> the secure function module further configured to receive a non-conforming computing module context that enables the secure function module to transact secure functions with a non-conforming computing module comprising storing cryptographic keys for the non-conforming computing module wherein the non-conforming computing module cannot transact the secure function with the secure function module using cryptographic keys of the excluding computing module;
>
> a communication module configured to communicate with the excluding computing module, **the excluding computing module configured to exclusively transact the secure function with the secure function module so that the non-conforming computing module must transact the secure function through the excluding computing module**, the communication module further configured to communicate with the non-conforming computing module, **the non-conforming**

**computing module configured to transact the secure function with the secure function module and unable to transact the secure function through the excluding computing module**; and

a context module configured to identify the excluding computing module initiating the secure function and set the context of the secure function module to the excluding computing module context and to identify the non-conforming computing module initiating the secure function and set the context of the secure function module to the non-conforming computing module context."

Independent claims 8, 11, 17, 24, and 30 include similar limitations. The present invention provides for both an excluding computing module and a non-conforming computing module to access a TPM. The excluding computing module is designed to exclusively access the TPM, so that no other computing module, including a non-conforming computing module, may access the TPM except through the excluding computing module. Typically the excluding computing module is an operating system. The operating system typically allows other computing modules to access the TPM only through an operating system Application Program Interface (API).

The non-conforming computing module is typically a legacy application that was designed to access the TPM directly rather than through an API of the operating system. Thus the non-conforming computing module is unable to transact the secure function through the excluding module.

Applicants submit that the seeming contradiction pointed out by the Examiner is the real-world situation that is resolved by the present invention. The situation is outlined in the background of the invention. See page 2, ¶ 6-7. The present invention claims identifying either the excluding computing module or the non-conforming computing module and setting the context of a secure function module of the TPM accordingly so that either the excluding computing module or the non-conforming computing module may transact a secure function.

Applicants therefore submit that claims 1, 4-11, 14-17, 19-24, and 26-30 are definite

under 35 U.S.C. § 112, second paragraph as the limitations of the claims describe a valid, real-world situation and a definite invention that functions within that situation.

**Rejections Under 35 U.S.C. 103**

Claims 1, 4-11, 14-17, 19-24, and 26-30 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Ilnicki in view of Brickell. Applicants traverse this rejection.

Independent claim 1 includes the limitations:

> "…a secure function module configured to **receive an excluding computing module context that enables the secure function module to transact secure functions with an excluding computing module** comprising storing cryptographic keys for the excluding computer module;
>
> the secure function module further configured to **receive a non-conforming computing module context that enables the secure function module to transact secure functions with a non-conforming computing module** comprising storing cryptographic keys for the non-conforming computing module wherein the non-conforming computing module cannot transact the secure function with the secure function module using cryptographic keys of the excluding computing module;
>
> a communication module configured to communicate with the excluding computing module, **the excluding computing module configured to exclusively transact the secure function with the secure function module so that the non-conforming computing module must transact the secure function through the excluding computing module**, the communication module further configured to communicate with the non-conforming computing module, **the non-conforming computing module configured to transact the secure function with the secure**

**function module and unable to transact the secure function through the excluding computing module**; and

a context module configured to **identify the excluding computing module initiating the secure function and set the context of the secure function module to the excluding computing module context and to identify the non-conforming computing module initiating the secure function and set the context of the secure function module to the non-conforming computing module context**."

Independent claims 8, 11, 17, 24, and 30 include similar limitations. Ilnicki and Brickell do not teach both an exclusive computing module and a non-conforming computing module, the exclusive computing module configured so that the non-conforming computing module must transact the secure function with the secure function module through the exclusive computing module and the non-conforming computing module unable to transact the secure function with the secure function module using cryptographic keys of the excluding computing module. Instead, Ilnicki teaches securely transferring data between an application server and an agent using a session key. Ilnicki, Abstract. If the application server in combination with the TPM of Brickell is analogous to the TPM of the present invention, there is no teaching of the application server being limited to exclusively transacting a secure function with the agent. In addition, there is no non-conforming computing module in Ilnicki and Brickell that can also transact the secure function with the application server but that cannot transact the secure function with the application server through the agent.

In addition, Ilnicki and Brickell do not teach identifying the excluding computing module initiating the secure function and setting the context of the secure function module to the excluding computing module context, nor do Ilnicki and Brickell teach identifying the non-conforming computing module initiating the secure function and setting the context of the secure function module to the non-conforming computing module context. Instead Ilnicki discloses

transferring data from a non-secure environment to secure environment. Ilnicki, col. 10, lines 55-64.

Further, Ilnicki and Brickell do not disclose setting a context of a secure function module to the excluding computing module context when the excluding computing module is identified as initiating a secure function and setting the context of the secure function module to the non-conforming computing module context when the non-conforming computing module is identified as initiating the secure function. Ilnicki only teaches the single context of a conforming measuring agent communicating with the application server. Ilnicki, Abstract. Ilnicki does not disclose setting the excluding computing module context and the non-conforming computing module context. Brickell also only discloses the single context of a conforming challenger communicating with a single responder, and does not teach both the excluding computing module context and the non-conforming computing module context. Brickell, Abstract.

Applicants therefore submit that Ilnicki and Brickell do not disclose each element of claims 1, 8, 11, 17, 24, and 30, and that claims 1, 8, 11, 17, 24, and 30 are allowable. Applicants further submit that claims 4-7, 9, 10, 14-16, 19-23, and 26-29 are allowable as depending from allowable claims.

**Conclusion**

As a result of the presented remarks, Applicants submit that the application is in condition for allowance. In the event any questions remain, the Examiner is respectfully requested to initiate a telephone conference with the undersigned.

Respectfully submitted,

Date: August 26, 2008

/Brian C. Kunzler/

Kunzler & Associates
8 E. Broadway, Suite 600
Salt Lake City, Utah 84111
Telephone: 801/994-4646

Brian C. Kunzler
Reg. No. 38,527
Attorney for Applicant